IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

KYLIE S., individually and as legal guardian for her minor daughter K.S., individually and on behalf of all other similarly situated individuals,	)	Case No._____
Plaintiff,	)	**CLASS ACTION COMPLAINT**
v.	)	**JURY TRIAL DEMANDED**
PEARSON, plc, doing business as Pearson Clinical Assessments, and NCS Pearson, Inc.	)	**INJUNCTIVE RELIEF DEMANDED**
Defendants.	)	

CLASS ACTION COMPLAINT

Plaintiff Kylie S., individually and as legal guardian for her minor daughter K.S. ("Plaintiff"), by and through her attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Pearson plc, d/b/a Pearson Clinical Assessment ("Pearson Clinical"), and Defendant NCS Pearson, Inc. ("NCS") (Pearson Clinical and NCS collectively "Pearson" or "Defendants"), and makes the following allegations based upon knowledge as to herself and her own acts, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. In November 2018, Pearson failed to exercise reasonable care in securing and safeguarding the sensitive data stored in its AIMSweb 1.0 platform ("AIMSweb") of nearly one million students enrolled in approximately 13,000 schools in at least thirteen states across the United States resulting in the theft of that data (the "Data Breach). Among the data stolen was first and last names, dates of birth, email addresses and unique student identification numbers

(collectively, "PII"). Pearson failed to have available systems in place to detect the breach on its own. Only after the Federal Bureau of Investigation informed Pearson of the Data Breach in March 2019 did Pearson begin to take action to secure the student' data. Even then, Pearson concealed its knowledge of the breach from students and their guardians until July 2019 when Pearson Clinical finally notified impacted schools and released a public statement. In disclosing the Data Breach, Defendants concealed the true extent of the breach to minimize the impact on their reputations.

2. The Data Breach resulted from Defendants' failure to secure and protect the PII students were compelled to provide to Defendants. These students now have to live the rest of their lives knowing that criminals have the ability to compile, build and amass their profiles for decades – exposing them to a never-ending threat of identity theft, extortion, bullying and harassment.

3. Defendants disregarded the rights of Plaintiff and the Classes (defined below) by intentionally, willfully, recklessly or negligently: (a) failing to take adequate and reasonable measures to ensure the security of AIMSweb; (b) concealing or otherwise omitting the material fact that they did not have systems in place to safeguard student PII; (c) failing to take available steps to detect and prevent the Data Breach; (d) failing to monitor AIMSweb and to timely detect the Data Breach; and (e) failing to provide Plaintiff and the Classes prompt and accurate notice of the Data Breach.

4. As a result of Defendants' misconduct, the Data Breach compromised the PII of Plaintiff and Class Members and made it available to criminals for misuse. The injuries Plaintiff and Class Members suffered as a direct result of the Data Breach include:

a. theft of personal information;

b. costs associated with the detection and prevention of identity theft;

c. costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach such as time taken from the enjoyment of one's life, and the inconvenience, nuisance, cost and annoyance of dealing with all issues resulting from the Data Breach;

d. the imminent and certainly impending injury resulting from the potential fraud and identity theft posed by PII being exposed for theft and sale on the dark web;

e. damages to and diminution in value of the PII that Defendants were supposed to keep secure; and

f. the loss of Plaintiff's and Class Members' privacy.

5. Defendants directly and proximately caused the injuries Plaintiff and the Class suffered by failing to implement or maintain adequate data security measures for PII.

6. Defendants have acknowledged the injuries and certainly impending injuries caused by their actions by offering temporary credit monitoring services to all impacted students, which services do not and cannot prevent or rectify the full extent of injuries Plaintiff and Class Members have suffered and will suffer far into the future.

7. Plaintiff and Class Members retain a significant interest in ensuring that their PII, which remains in Defendants' possession, is protected from further breaches, and seek to remedy the harms suffered as a result of the Data Breach for themselves and on behalf of similarly situated persons whose PII was stolen.

8. Plaintiff, individually, and on behalf of similarly situated persons, seeks to recover damages, equitable relief, including injunctive relief designed to prevent a reoccurrence of the Data Breach and resulting injuries, restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

PARTIES

9. Plaintiff Kylie S., individually and as legal guardian for her daughter K.S., is an Illinois resident. K.S. attended a public school in Illinois that utilized AIMSweb. K.S.'s PII was compromised and stolen as a result of the Data Breach

10. Defendant Pearson plc is a for-profit, British corporation that does business throughout the United States with a principal place of business in San Antonio, Texas. At relevant times, Pearson plc, doing business as Pearson Clinical Assessment, had responsibility for AIMSweb. As recently as 2017, *Publisher's Weekly* listed Pearson as the largest publisher in the world. Pearson plc holds itself out as the "world's learning company" and operates in dozens of counties worldwide, including all fifty states in the United States of America. Pearson plc provides content, assessment and digital services to schools and seeks to grow its market share through digital transformation. As of December 2018, Pearson plc reported total assets of approximately $9.683 billion.

11. Defendant NCS Pearson, Inc. is a Minnesota corporation with its principal place of business in Bloomington, Minnesota. NCS Pearson, Inc. is a wholly-owned subsidiary of Pearson plc. NCS Pearson, Inc. operates in the United States and markets application software for education, testing, assessment and complex data management. NCS Pearson, Inc. had responsibility for AIMSweb at relevant times.

JURISDICTION AND VENUE

12. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) (the "Class Action Fairness Act") because sufficient diversity of citizenship exists between parties in this action, the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, and there are 100 or more members of the Classes, based on published news reports of the impacts of the Data Breach. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

13. This Court has personal jurisdiction over Defendants because they are authorized to do business in this District and regularly conduct business in this District, have sufficient minimum contacts with this state and/or sufficiently avail themselves of the markets of this state through their promotion, sales, licensing and marketing within this state.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) and (2) because the unlawful conduct alleged in this Class Action Complaint occurred in, was directed to and/or emanated in part from this District.

FACTUAL ALLEGATIONS

I. Data Breaches and the Market for PII.

15. Data breaches in the United States have become commonplace – almost 2,900 between 2017 and 2018 – with the goal of criminals being to monetize stolen data.[1]

16. When a victim's data is compromised in a breach, the victim is exposed to serious ramifications regardless of the sensitivity of the data.[2]

[1] Identity Theft Resource Center, 2017 Annual Data Breach Year-End Review, available at https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf (last accessed on August 22, 2019).
[2] *Id.*

17. According to Javelin Strategy & Research, in 2017 over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.

18. The problem is compounded when companies entrusted with people's data fail to implement industry best practices because cyberattacks and other data exploitations can go undetected for a long period of time.

19. A person's identity is akin to a puzzle – the more accurate pieces a thief obtains about someone, the more the thief can take on the identity of the person and use software to figure out the person's passwords.[3] Armed with just an email address and password, a data thief can change a person's passwords, lock a person out of her online accounts and obtain additional sensitive PII.[4]

20. PII is a valuable commodity for which a black market exists on the dark web, among other places. In this black market, criminals seek to sell the spoils of their cyberattacks to identity thieves who desire the data to extort and harass victims, take over victims' identities in order to open financial accounts and otherwise engage in illegal financial transactions under the victims' names.

21. PII has a defined value – which is why legitimate companies and criminals seek to obtain and sell it. As alleged in more detail below, a growing market is for children's data.[5]

22. The U.S. Department of Justice's Bureau of Justice Statistics has found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that resolution of those problems could take more than a year.[6]

---

[3] *Id.*
[4] *Id.*
[5] *The Worrying Trend of Children's Data Being Sold on the Dark Web*, available at https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark-web/ (last accessed on August 22, 2019).

23. The U.S. Government Accountability Office has concluded that it is common for data thieves to hold onto stolen data for extended periods of time before utilizing it for identity theft.[7] In the same report, the Government Accountability Office noted that while credit monitoring services can assist with detecting fraud, those services do not stop it.[8]

II. The Unique Nature of Student Data Commands Extra Vigilance in Protecting It.

24. Education technology platforms are popular targets for cyberattacks given the young age and vulnerability of the victims and the sensitive nature of the data stored therein.

25. Criminals increasingly seek out children's data because children are less likely to check their credit reports or implement credit freezes, giving criminals longer periods of time to utilize a child's stolen identity.[9]

26. The FBI has warned that "widespread collection of student data could have privacy and safety implications if compromised or exploited."[10] According to the FBI, malicious use of sensitive student data "could result in social engineering, bullying, tracking, identity theft, or other means for targeting children."[11]

---

[6] U.S. Department of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2014* (Sept. 2015), available at http://www.bjs.gov/content/pub/pdf/vit14.pdf (last accessed on August 25, 2019).
[7] U.S. Government Accountability Office Report to Congressional Requesters, *Data Breaches – Range of Consumer Risks Highlights Limitations of Identity Theft Services*, available at https://www.gao.gov/assets/700/697985.pdf (last accessed on August 25, 2019).
[8] *Id.*
[9] *See The Worrying Trend of Children's Data Being Sold on the Dark Web*, available at https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark-web/ (last accessed on August 22, 2019).
[10] *Education Technologies: Data Collection and Unsecured Systems Could Pose Risks to Students*, FBI Alert No. I-091318-PSA (Sept. 13, 2018), available at https://www.ic3.gov/media/2018/180913.aspx (last accessed on August 22, 2019).
[11] *Id.*

27. Three United States Senators recently expressed growing concern over stories and warnings involving breaches involving student data.[12] According to the Senators, a particularly alarming aspect of student data breaches is the fact that "students have little control over how their data is being collected and used. Students and parents are often unaware of the amount and type of data being collected about them and who may have access to it."[13]

28. Due to the special risks associated with student data breaches and the increasing frequency with which they are occurring, it is imperative for education technology companies like Pearson to routinely: (a) monitor for system breaches, cyberattacks and other exploitations; and (b) update their software, security procedures and firewalls.

III. The Data Breach.

27. AIMSweb was a digital education technology assessment platform licensed to schools by Defendants.

28. Students who were enrolled in a school that utilized AIMSweb were subjected to the AIMSweb assessments as part of the school's regular curriculum.

29. At relevant times, Plaintiff and Class Members took reasonable steps to safeguard their PII.

30. Nevertheless, merely by attending school, Plaintiff and Class Members were compelled to provide Defendants valuable and sensitive PII, including their first and last names, dates of birth, email addresses and unique student identification numbers.

[12] A copy of one of the letters sent by the U.S. Senators to education technology companies is available at https://www.durbin.senate.gov/newsroom/press-releases/durbin-markey-blumenthal-request-information-on-student-data-collection-practices (last accessed on August 22, 2019).
[13] *Id.*

31. Plaintiff and Class members as captive users of AIMSweb relied on Defendants to keep their PII confidential and securely maintained, to solely use the information for educational purposes and to make only authorized disclosures of the information.

32. Notwithstanding the regularity with which data breaches were occurring in the United States and the FBI's concern with respect to student data, Defendants did not take the necessary steps to ensure that AIMSweb was secure and safe from cyberattack.

33. In March 2019, the FBI notified Defendants of a November 2018 cyberattack on AIMSweb that impacted approximately 13,000 school accounts containing the data of hundreds of thousands of students across the United States.

34. At no time between November 2018 and March 2019 did Defendants detect the cyberattack or Data Breach on their own or take any steps to fix the vulnerability that allowed for the breach.

35. Even after learning of the Data Breach in March 2019, Defendants concealed that fact from impacted schools for four months, failing to disclose it until late July 2019.

36. Defendants kept the Data Breach concealed from the public-at-large even longer – delaying public notification until July 31, 2019.

37. When Defendants finally gave notice of the Data Breach, they concealed the true extent and gravity of the breach.

38. For instance, a notice issued by Pearson Clinical represented that the Data Breach was "isolated to first name, last name, and in some instances may include date of birth and/or email address,"[14] whereas in fact: (a) the Data Breach exposed other sensitive student data including students' unique student identification numbers; and (b) the extent of disclosed of dates of birth and email addresses was far greater than Pearson Clinical represented.

[14] Data Breach notification provided to impacted schools.

39. Moreover, Pearson Clinical claimed that it did not "have any evidence that this information has been misused" and was disclosing the Data Breach merely to "bring this to your attention as a precaution."[15]

40. While Defendants downplayed the extent and gravity of the Data Breach, at the same time, it tacitly acknowledged the actual and certainly imminent injuries suffered by victims of the Data Breach by offering such victims one year of complimentary credit monitoring services.

41. The offered credit monitoring services do not sufficiently protect the students subjected to the Data Breach from the threats posed thereby and are not in effect long enough to eliminate all potential damage from the Data Breach.

IV. Defendants' Duty to Safeguard Student Data.

42. By obtaining, collecting, using and deriving a benefit from Plaintiff and the Class Members' PII, Defendants assumed legal and equitable duties to those individuals, including the duty to protect Plaintiff and Class Members' PII from disclosure.

43. Beyond Defendants' legal obligations to protect the confidentiality of students' PII, at relevant times, Pearson Clinical affirmatively represented that it would safeguard their privacy:

> When you share your personal information with any company, you have a right to expect that information to be treated with total confidentiality.
>
> Your privacy is extremely important to us. We're committed to protecting any personal information you've given us, and we comply with all relevant data protection laws.
>
> * * *
>
> At Pearson, we know that you care how your personal information is used and we appreciate that you trust us to do that carefully and sensibly.[16]

[15] *Id.*

44. At relevant times, Defendants knew the importance of safeguarding the student PII with which it was entrusted and the foreseeable consequences – and ensuing significant injuries – in the event of an AIMSweb data breach.

45. At relevant times, Defendants were aware or reasonably should have been aware that the PII collected, maintained and stored within AIMSweb was highly sensitive, susceptible to attack and, if improperly obtained, could be used by third parties for wrongful purposes such as identity theft and fraud.

46. At relevant times, Defendants knew, or reasonably should have known, of the significant volume of student data they received on a regular basis and the corresponding number of students who would be harmed by an AIMSweb breach.

47. At relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding PII, and of the foreseeable consequences that would occur in the event of an AIMSweb breach, including the significant cost that students would incur as a result of any breach.

48. Notwithstanding all of the publicly-available information and knowledge regarding cyberattacks on education technology vendors and the corresponding dangers to students, Defendants were negligent or reckless in their approach to safeguarding the data stored within AIMSweb and the privacy of the students' data stored therein.

[16] Pearson Clinical Privacy Notice, available at https://www.pearson.com/corporate/privacy-notice.html (last accessed on August 25, 2019).

V. Defendants Failed to Comply with Federal Requirements

49. The Federal Trade Commission ("FTC") has instructed that the need for data security should be factored into all business decision-making.[17] To that the end, the FTC recommends that companies verify that third-party service providers have reasonable security measures in place; timely dispose of PII that is no longer needed; require the use of complex passwords on networks and monitor for suspicious activity thereon; and implement security methods that have been industry-tested.[18]

50. According to published FTC guidelines, businesses should: (a) protect customers' personal information – including encrypting information stored on computer networks and implementing policies to address security issues; (b) properly dispose of customer information when it is no longer needed; and (c) understand vulnerabilities on their network.[19] According to the guidelines, businesses should also have systems in place to detect intrusions and expose breaches as soon as they occur.

51. Pursuant to Section 5 of the FTC Act (15 U.S.C. § 45), the FTC has brought numerous actions against businesses for their failure to protect customer data, alleging that the conduct constitutes an unfair act or practice. The dispositions of these actions further inform the obligations of businesses when it comes to data security.

52. At relevant times, Defendants knew of their obligation to protect customer PII – especially given the fact that they were handling the PII of children – as well as the consequences of their failure to do so.

---

[17] Federal Trade Commission, *Start With Security,* available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed on August 28, 2019).

[18] *Id.*

[19] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed on August 28, 2019).

53. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to customers PII constitutes and unfair act or practice in violation of the FTC Act.

VI. Plaintiff and Class Members' Injuries and Damages.

54. As a result of the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer severe consequences, as they are more likely to become victims of social engineering,[20] bullying, tracking, identity theft, and other means of targeting.

55. Defendants' failure to timely detect and deliberate delay in notifying students of the Data Breach increased the risks and consequences Plaintiff and Class Members will suffer as a result of the Data Breach because cybercriminals had a head start to use the stolen data for their benefit and to the detriment of Plaintiff and Class Members.

56. In order to prevent or limit the possibility of misuse of their PII, Plaintiff and Class Members will have to take the following steps, among others:

a. Place a fraud alert on their credit bureau reports;

b. Place a security freeze on their credit bureau reports;

c. Periodically monitor their credit bureau reports for any unusual activity; and

d. Obtain new student identification numbers and change email addresses and account passwords.

57. Because data thieves often delay using stolen information, Plaintiff and Class Members will continue to be at risk of the above-alleged harms well into the future.

[20] Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing confidential or personal information. The more information a data thief has about an individual, the better chance he/she has of obtaining confidential information.

58. Defendants' wrongful actions and inaction have directly and proximately caused Plaintiff and Class Members to face the immediate and continuing increased risk of economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of personal information;

b. costs associated with the detection and prevention of identity theft;

c. costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach such as time taken from the enjoyment of one's life, and the inconvenience, nuisance, cost and annoyance of dealing with all issues resulting from the Data Breach;

d. the imminent and certainly impending injury resulting from the potential fraud and identity theft posed by PII being exposed for theft and sale on the dark web;

e. damages to and diminution in value of the PII that Defendants were supposed to keep secure; and

f. the loss of Plaintiff's and Class Members' privacy.

CLASS ACTION ALLEGATIONS

59. Plaintiff brings this action on behalf of herself and a class action under Federal Rules of Civil Procedure 23, seeking damages and equitable relief on behalf of the following nationwide Class for which Plaintiff seeks certification:

> All persons residing in the United States who used or utilized AIMSweb and whose PII was accessed without authorization as a result of the Data Breach (the "Nationwide Class").

60. Additionally, Plaintiff brings this action on behalf of a state subclass seeking damages and equitable relief on behalf of the following:

> All persons residing in the State of Illinois who used or utilized AIMSweb and whose PII was accessed without authorization as a result of the Data Breach (the "Illinois Subclass").

61. Excluded from the Classes are Pearson plc; NCS Pearson, Inc.; any parent, affiliate or subsidiary Pearson plc or NCS Pearson, Inc.; any entity in which Pearson plc or NCS Pearson, Inc. has a controlling interest; any of Pearson plc or NCS Pearson, Inc.'s officers or directors; or any successor or assign of Pearson plc or NCS Pearson, Inc. Also excluded are any judge or court personnel assigned to this case and members of their immediate families.

62. Plaintiff reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

63. **Numerosity.** Consistent with Rule 23(a)(1), the Classes are so numerous that joinder of all members is impracticable. While Plaintiff does not know the exact number of the members of the Classes, Plaintiff believes the Nationwide Class contains hundreds of thousands of people. Class Members may be identified through objective means, including objective data available to Defendants regarding whose data was accessed without authorization as a result of the Data Breach. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, social media and/or published notice. All members of the Nationwide Class and Illinois Subclass are readily ascertainable because Defendants have access to information regarding the identity of each AIMSweb user.

64. **Commonality and predominance.** Common questions of law and fact exist as to all Class Members. These common questions of law or fact predominate over any questions affecting only individual members of the Classes. Common questions include, but are not limited to the following:

a. Whether Defendants engaged in wrongful conduct as alleged herein;

b. Whether Defendants owed a duty to Plaintiff and Class Members to adequately protect their PII and to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members and whether Defendants willfully, recklessly or negligently breached these duties;

c. Whether Defendants willfully, recklessly or negligently failed to maintain and execute reasonable procedures to prevent unauthorized access to their data security networks and to Plaintiff and Class Members' PII;

d. Whether Defendants' conduct – including their failure to act – resulted in or was the proximate cause of the Data Breach;

e. Whether Defendants failed to inform Plaintiff and Class Members of the Data Breach in a timely and accurate manner;

f. Whether Defendants continue to breach their duties to Plaintiff and Class Members;

g. Whether Defendants have sufficiently addressed or remedied Plaintiff and Class Members' injuries and have taken adequate preventive and precautionary measures to ensure that Plaintiff and Class Members will not experience further harm;

h. Whether Defendants' security measures to protect its computer systems were reasonable in light of the FTC data security recommendations and best practices recommended by security experts.

i. Whether Defendants failed to protect Plaintiff and Class Members by allowing unauthorized access to their PII.

j. Whether Defendants engaged in unfair or deceptive trade practices by failing to disclose that they failed to properly safeguard Plaintiff and Class Members' PII;

k. Whether Plaintiff and Class Members suffered damages as a proximate result of Defendants' conduct or failure to act; and

l. Whether Plaintiff and Class Members are entitled to damages, equitable relief and other relief.

65. **Typicality.** Plaintiff's claims are typical of the claims of the Nationwide Class and Illinois Subclass she seeks to represent because Plaintiff and all members of the proposed Nationwide Class and Illinois Subclass have suffered similar injuries as a result of the same practices alleged herein. Plaintiff has no interests to advance adverse to the interests of the other members of the Nationwide Class and Illinois Subclass.

66. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the Nationwide Class and Illinois Subclass and has retained as her counsel attorneys experienced in class actions and complex litigation.

67. **Superiority.** A class action is superior to other available means for the fair and efficient adjudication of this dispute. The injury suffered by each Class Member, while meaningful on an individual basis, is not of such magnitude as to make the prosecution of individual actions against Defendants economically feasible. Even if Class Members could afford individual litigation, those actions would put immeasurable strain on the court system. Moreover, individual litigation of the legal and factual issues of the case would increase the delay and expense to all parties and the court system. A class action, however, presents far fewer

management difficulties and provides the benefit of single adjudication, economy of scale and comprehensive supervision by a single court.

68. In the alternative, the proposed classes may be certified because:

a. The prosecution of separate actions by each individual member of the Nationwide Class and Illinois Subclass would create a risk of inconsistent adjudications, which could establish incompatible standards of conduct for Defendants;

b. The prosecution of individual actions could result in adjudications that as a practical matter would be dispositive of the interests of non-party Class Members or which would substantially impair their ability to protect their interests; and

c. Defendants acted or refused to act on grounds generally applicable to the proposed classes, thereby making appropriate final and injunctive relief with respect to members of the Nationwide Class and Illinois Subclass as a whole.

69. Pursuant to Rule 23(c)(4) particular issues are appropriate for certification – namely the issues described in paragraph 64, above, because resolution of such issues would advance the disposition of the matter and the parties' interests therein.

CLAIMS FOR RELIEF

COUNT ONE
NEGLIGENCE
(On behalf of all Classes)

70. Plaintiff restates and realleges paragraphs 1 through 69, above, as though fully set forth herein.

71. Defendants obtained Plaintiff and Class Members' PII and had a duty to exercise reasonable care in securing that information from unauthorized access or disclosure.

72. Defendants also had a duty to destroy Plaintiff and Class Members' PII within an appropriate amount of time after it was no longer required by Defendants, in order to mitigate the risk of the stale PII being compromised in a data breach.

73. Further, Defendants had a duty to adequately protect AIMSweb and the PII stored thereon.

74. Once in possession and custody of Plaintiff and Class Members' PII within AIMSweb, Defendants undertook and owed a duty of care to Plaintiff and Class Members to exercise reasonable care to secure and safeguard Plaintiff and Class Members' PII – which they knew was private and confidential and should be protected as such – and to use commercially-reasonable methods to do so.

75. Defendants owed a duty of care not to subject Plaintiff and Class Members' PII or Plaintiff and Class Members themselves to an unreasonable risk of harm from a data breach because Plaintiff and Class Members were foreseeable and probable victims of inadequate security practices.

76. Defendants owed a duty of care to Plaintiff and Class Members to quickly detect a data breach and to timely act on data breach warnings.

77. Defendants owed a duty to Plaintiff and Class Members to timely and accurately disclose the Data Breach and the nature thereof.

78. Defendants' duties arose from their relationship to Plaintiff and Class Members, out of their possession and custody of Plaintiff and Class Members' PII and from industry custom.

79. Through their actions and/or failures to act, Defendants unlawfully breached duties owed to Plaintiff and Class Members by failing to implement standard industry protocols and failing to exercise reasonable care to secure and keep private the PII entrusted to it, including allowing unauthorized access to PII and failing to provide adequate oversight over the PII with which Defendants were entrusted despite knowing the foreseeable risk and likelihood of a data breach which would allow unauthorized third parties unfettered access to and use of Plaintiff and Class Members' PII without consent.

80. Through their actions and/or failures to act, Defendants allowed unmonitored and unrestricted access to unsecured PII.

81. Through their actions and/or failures to act, Defendants failed to provide adequate supervision and oversight of the PII with which they were entrusted, despite knowing the risk and foreseeable likelihood of a breach and misuse, which permitted unknown third parties to gather Plaintiff and Class Members' PII, misuse that PII and intentionally disclose it without consent.

82. Based on the publicity surrounding data breaches, at relevant times, Defendants knew or should have known the risks inherent in obtaining, collecting and storing PII and the concomitant necessity for adequate security measures to protect that PII.

83. At relevant times Defendants knew or should have known that AIMSweb and related systems failed to adequately safeguard Plaintiff and Class Members' PII, thereby creating a foreseeable risk that unauthorized third parties could and would gain access to Plaintiff and Class Members' PII.

84. Due to Defendants' knowledge that a breach of AIMSweb and related systems would damage hundreds of thousands of students, including Plaintiff and Class Members, Defendants had a duty to adequately protect AIMSweb and the PII contained thereon.

85. Defendants had a special relationship with Plaintiff and Class Members. Plaintiff and Class Members were compelled to entrust Defendants with their PII. At relevant times, Plaintiff and Class Members understood that AIMSweb would take adequate security precautions to safeguard that information. Only Defendants had the ability to protect from attack AIMSweb and the PII stored on AIMSweb and related systems.

86. Defendants' own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their PII. Defendants' misconduct included failing to: (a) secure its computer systems, despite knowing their vulnerabilities; (b) comply with industry standard security practices; (c) implement adequate system and event monitoring; and (d) implement the systems, policies and procedures necessary to prevent this type of data breach.

87. Defendants breached the above-alleged duties to Plaintiff and Class Members by, among other things: (a) failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Plaintiff and Class Members' PII; (b) creating a foreseeable risk of harm through the above-alleged misconduct; (c) failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff and Class Members' PII before and after learning of the Data Breach; (d) failing to utilize measures and practices that would allow

for the timely detection of a data breach or other unauthorized access to PII within AIMSweb; (e) failing to comply with industry data security standards during the period of the Data Breach; and (f) failing to timely and accurately disclose that Plaintiff and Class Members' PII had been improperly acquired or accessed.

88. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of Plaintiff and Class Members' PII, so that Plaintiff and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

89. Defendants breached their duty to notify Plaintiff and Class Members of the unauthorized access to their PII by waiting to notify Plaintiff and Class Members, and then by failing to provide Plaintiff and Class Members with sufficient or accurate information regarding the Data Breach.

90. Through Defendants' acts and omissions described herein, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiff and Class Members' PII while it was within Defendants' possession or control.

91. On information and belief, Defendants improperly and inadequately safeguarded Plaintiff and Class Members' PII in deviation of standard industry rules, regulations and practices at the time of the unauthorized access. Defendants' failure to take proper security measures to protect sensitive PII as described herein created conditions conducive to a foreseeable, intentional criminal act – namely the unauthorized access of Plaintiff and Class Members' PII.

92. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including but not limited to: (a) failing to adequately protect the PII; (b) failing

to conduct regular security audits; (c) failing to provide adequate and appropriate supervision of persons having access to Plaintiff and Class Members' PII; and (d) failing to provide Plaintiff and Class Members with timely and sufficient notice that their sensitive PII had been compromised.

93. Neither Plaintiff nor the other Class Members contributed to the Data Breach and subsequent misuse of their PII as described herein.

94. Defendants' failure to exercise reasonable care in safeguarding PII by adopting appropriate security measures, including proper encryption storage techniques, was the direct and proximate cause of Plaintiff and Class Members' PII being accessed and stolen through the Data Breach.

95. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable and adequate computer systems and data security practices to safeguard Plaintiff and Class Members' PII.

96. As a direct and proximate result of Defendants' breach of duties, Plaintiff and Class Members suffered damages including, but not limited to: (a) damages from lost time and the effort required to mitigate the actual and potential impact of the Data Breach on their lives, including by closely reviewing and monitoring their credit reports; and (b) damages from identity theft, which may take months, if not years, to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT TWO
(NEGLIGENCE *PER SE*)
(On behalf of all Classes)

97. Plaintiff restates and realleges paragraphs 1 through 69, above, as though fully set forth herein.

98. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including the unfair act or practice by businesses of failing to use reasonable measures to protect PII. The FTC publications and dispositions alleged above further define Defendants' duty under the FTC Act.

99. As alleged herein, Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards. Defendants' conduct was particularly unreasonable given the volume of PII it obtained and stored and the fact that much of the data was collected from students. The consequences of a data breach – including the damages Plaintiff and Class Members would suffer – were foreseeable to Defendants.

100. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

101. Plaintiff and Class Members are within the class of persons the FTC Act is intended to protect.

102. The harm that occurred as a result of the Data Breach is within the FTC's jurisdiction. As alleged herein, the FTC has brought enforcement actions against businesses that, like Defendants here, have failed to employ reasonable data security measures and engaged in unfair and deceptive practices, resulting in the same harm suffered by Plaintiff and Class Members.

103. As a direct and proximate result of Defendants' breach of duties, Plaintiff and Class Members suffered damages including, but not limited to: (a) damages from lost time and the effort required to mitigate the actual and potential impact of the Data Breach on their lives, including by closely reviewing and monitoring their credit reports; and (b) damages from identity theft, which may take months, if not years, to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

104. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to implement appropriate and adequate measures to protect that PII. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT THREE
(BREACH OF EXPRESS CONTRACT)
(On behalf of all Classes)

105. Plaintiff restates and realleges paragraphs 1 through 69, above, as though fully set forth herein.

106. Plaintiff and Class Members' use of AIMSweb was permitted pursuant to a standard licensing agreement (the "Express Contract") entered into between NCS and the schools at which Plaintiff and Class Members attended. As consideration, the various schools paid fees to NCS in return for use of AIMSweb. Plaintiff and Class Members are third-party beneficiaries of the Express Contract entered into by and between the school they attended and NCS, as the

purpose of the Express Contract was to enhance Plaintiff and Class Members' educational performance.

107. Pursuant to the Express Contract, NCS was to take reasonable actions to ensure that the PII of Plaintiff and Class Members' PII was only disclosed to those authorized parties.

108. On information and belief, each school attended by Plaintiff or Class Members fully performed its obligations under the Express Contract.

109. NCS breached the Express Contract by failing to employ reasonable and adequate privacy practices and measures, resulting in the disclosure of the PII of Plaintiff and Class Members for purposes not required or permitted under the Express Contract.

110. As a direct and proximate result of NCS' breaches of the Express Contract, Plaintiff and Class Members sustained actual losses as alleged above.

111. Plaintiff and Class Members suffered harm as a result of NCS' breach of the Express Contract because their PII was compromised, placing Plaintiff and Class Members at a greater risk of social engineering, bullying, tracking, identity theft, or other means of being targeted; and because their PII was disclosed to unauthorized third parties without their consent. Additionally, the value of Plaintiff and Class Members' PII has been diminished in that it is now in the hands of unauthorized third parties who can post it on the dark web or otherwise utilize it for their own interests.

112. NCS' breach of the Express Contract was a direct and legal cause of Plaintiff and Class Members' injuries and damages as alleged above.

COUNT FOUR
BREACH OF IMPLIED CONTRACT
(On behalf of all Classes)

113. Plaintiff restates and realleges paragraphs 1 through 69, above, as though fully set forth herein.

114. Defendants invited Plaintiff and Class Members to use AIMSweb to improve their educational advancement, in part, by providing their PII. Plaintiff and Class Members accepted Defendants' offer and provided their PII to Defendants.

115. When Plaintiff and Class Members provided their PII to Defendants in return for the purported benefits of AIMSweb, Plaintiff and Class Members, on the one hand, and Defendants, on the other, entered into mutually agreed-upon implied contracts pursuant to which Defendants agreed to utilize Plaintiff and Class Members' PII solely for the agreed-upon purpose of advancing their education.

116. In agreeing to solely use Plaintiff and Class Members' PII for the agreed-upon purpose of advancing Plaintiff and Class Members' education, Defendants further agreed they would use reasonable measures to safeguard Plaintiff and Class Members' PII.

117. Plaintiff and Class Members fully performed their obligations under the implied contracts alleged above.

118. Defendants breached the implied contracts alleged above by failing to employ reasonable and adequate privacy practices and measures, resulting in the disclosure of the PII of Plaintiff and Class Members for purposes not required or permitted under the implied contracts.

119. Defendants further breached the implied contracts alleged above by failing to provide timely and accurate notice to Plaintiff and Class Members that their PII was compromised as a result of the Data Breach.

120. Defendants further breached the implied contracts alleged above by failing to ensure that the PII of Plaintiff and Class Members was only used for the agreed-upon purpose of advancing their education.

121. As a direct and proximate result of Defendants' breaches of the implied contracts alleged above, Plaintiff and Class Members sustained actual losses as alleged above.

122. Plaintiff and Class Members suffered harm as a result of Defendants' breach of the implied contracts alleged above because their PII was compromised, placing Plaintiff and Class Members at a greater risk of social engineering, bullying, tracking, identity theft, or other means of being targeted; and because their PII was disclosed to unauthorized third parties without their consent. Additionally, the value of Plaintiff and Class Members' PII has been diminished in that is now in the hands of unauthorized third parties who can post it on the dark web or otherwise utilize it for their own interests.

123. Defendants' breach of the implied contracts alleged above was a direct and legal cause of Plaintiff and Class Members' injuries and damages as alleged above.

COUNT FIVE
UNJUST ENRICHMENT
(On behalf of all Classes)

124. Plaintiff restates and realleges paragraphs 1 through 69, above, as though fully set forth herein.

125. Plaintiff and Class Members conferred a monetary benefit on Defendants – namely, they provided and entrusted their PII to them.

126. In exchange, Plaintiffs and Class Members should have been entitled to have Defendants protect their PII with adequate data security.

127. Defendants appreciated, accepted and retained the benefit bestowed upon it under inequitable and unjust circumstances arising from Defendants' conduct toward Plaintiff and Class Members as described herein – namely, (a) Plaintiff and Class Members conferred a benefit on Defendants, and Defendants accepted or retained that benefit; and (b) Defendants used Plaintiff and Class Members' PII for business purposes.

128. Defendants failed to secure Plaintiff and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

129. Defendants acquired the PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged, as well as failed to destroy or otherwise purge the PII from AIMSweb and related systems after Defendants no longer had a legitimate business purpose to maintain that PII.

130. Plaintiff and Class Members have no adequate remedy at law.

131. Under the circumstances, it would be unjust and unfair for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred on them.

132. Under the principles of equity and good conscience, Defendants should not be permitted to retain the PII belonging to Plaintiff and Class Members because Defendants failed to implement the data management and security measures that industry standards mandate.

133. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from the use of Plaintiff and Class Members' PII.

COUNT SIX
INTRUSTION UPON SECULUSION
(On behalf of all Classes)

134. Plaintiff restates and realleges paragraphs 1 through 69, above, as though fully set forth herein.

135. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to protection of this information against disclosure to unauthorized third parties.

136. Defendants owed a duty to AIMSweb users, including Plaintiff and Class Members, to keep their PII confidential.

137. Defendants failed to protect Plaintiff and Class Members' PII stored within AIMSweb and related systems and released it to unknown and unauthorized third parties.

138. By way of Defendants' failure to protect the PII in AIMSweb and related databases, Defendants allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and Class Members.

139. The unauthorized release to, custody of and examination by unauthorized third parties of the PII of Plaintiff and Class Members – especially where the information includes dates of birth and student identification numbers and relates to children – is highly offensive to a reasonable person.

140. The intrusion was into a place or thing that was private and entitled to be private. While Plaintiff and Class Members were compelled to disclose their PII to Defendants as part of their use of Defendants' services, at all times the PII was supposed to be kept confidential and protected from unauthorized disclosure. It was reasonable for Plaintiff and Class Members to

believe that such information would be kept private and confidential and would not be disclosed without their authorization.

141. The Data Breach at the hands of Defendants constitutes an unauthorized intrusion or prying into Plaintiff and Class Members' seclusion, and the intrusion was of a kind that would be highly offensive to a reasonable person.

142. Defendants acted with a knowing state of mind when it permitted the Data Breach because it had actual knowledge that its information security practices were inadequate and insufficient.

143. As a proximate result of the above acts and omissions of Defendants, the PII of Plaintiff and Class Members was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer damages, anguish and suffering.

144. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendants can be viewed, distributed and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

COUNT SEVEN
ILLINOIS PERSONAL INFORMATION AND PROTECTION ACT
815 ILCS 530/1, *et seq.*
(On behalf of the Illinois Subclass)

145. Plaintiff restates and realleges paragraphs 1 through 69, above, as though fully set forth herein.

146. As corporations that handle, collect, disseminate and otherwise deal with nonpublic personal information, Defendants are Data Collectors as defined in 815 ILCS 530/5.

147. By failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay, Defendants violated 815 ILCS § 530/10(a).

148. Pursuant to 815 ILCS § 530/20, a violation of 815 ILCS § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

149. As a direct and proximate result of Defendants' violations of 815 ILCS § 530/10(a), Plaintiff and Illinois Subclass Members suffered damages, as described above.

150. Plaintiff and Illinois Subclass Members seek relief under 815 ILCS § 505/10a for the harm they suffered because of Defendants' willful violations of 815 ILCS § 530/10(a), including actual damages, restitution, punitive damages, injunctive relief and reasonable attorneys' fees and costs.

COUNT EIGHT
ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT
815 ILCS 505/1, *et seq.*
(On behalf the Illinois Subclass)

151. Plaintiff restates and realleges paragraphs 1 through 69, above, as though fully set forth herein.

152. Each Defendant is a "person" as defined by 815 ILCS § 505/1(c).

153. Defendants' conduct as alleged herein was in the conduct of "trade" or "commerce" as defined by 815 ILCS § 505/1(f).

154. Defendants' deceptive, unfair and unlawful trade acts or practices, in violation of 815 ILCS § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Illinois Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and Illinois Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to security and privacy of Plaintiff and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS § 510/2(a);

f. Omitting, suppressing and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Illinois Subclass Members' PII; and

g. Omitting, suppressing and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass Members' PII, including

duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS § 510/2(a).

155. Defendants' representations and omissions were material because they were likely to deceive reasonable persons about the adequacy of Defendants' data security and ability to protect the confidentiality of persons' PII.

156. Defendants intended to mislead Plaintiff and Illinois Subclass Members and induce them to rely on their misrepresentations and omissions.

157. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive and unscrupulous. These acts caused substantial injury to Plaintiff and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to competition.

158. Defendants acted intentionally, knowingly and maliciously to violate Illinois' Consumer Fraud and Deceptive Business Practices Act and recklessly disregarded Plaintiff and Illinois Subclass Members' rights.

159. As a direct and proximate result of Defendants' unfair, unlawful and deceptive practices and acts, Plaintiff and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property and monetary and non-monetary damages, including from fraud and identity theft; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

160. Plaintiff and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief and reasonable attorneys' fees and costs.

COUNT NINE
ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT
815 ILCS 510/1, *et seq.*
(On behalf the Illinois Subclass)

161. Plaintiff restates and realleges paragraphs 1 through 69, above, as though fully set forth herein.

162. Each Defendant is a "person" as defined by 815 ILCS § 510/1(5).

163. Defendants engaged in deceptive trade practices in the conduct of their businesses in violation of 815 ILCS § 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in conduct that creates a likelihood of confusion or misunderstanding.

164. Defendants' deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Illinois Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to security and privacy of Plaintiff and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and Illinois Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to security and privacy of Plaintiff and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS § 510/2(a);

f. Omitting, suppressing and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Illinois Subclass Members' PII; and

g. Omitting, suppressing and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 ILCS § 510/2(a).

165. Defendants' representations and omissions were material because they were likely to deceive reasonable persons about the adequacy of Defendants' data security and ability to protect the confidentiality of persons' PII.

166. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive and unscrupulous. These acts caused substantial injury to Plaintiff and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to competition.

167. As a direct and proximate result of Defendants' unfair, unlawful and deceptive trade practices, Plaintiff and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property and monetary and non-monetary damages, including from fraud and identity theft; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

168. Plaintiff and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and as legal guardian for her minor daughter, on behalf of her herself, her minor daughter and the Classes, respectfully seeks from the Court the following relief:

a. Certification of the Classes as requested herein;

b. Appointment of Plaintiff as Class representative and her undersigned counsel as Class counsel;

c. Award Plaintiff and members of the proposed Classes damages;

d. Award Plaintiff and members of the proposed Classes equitable, injunctive and declaratory relief, including the enjoining of Defendants' insufficient data protection practices at issue herein and Defendants' continuation of their unlawful business practices as alleged herein;

e. An order declaring that Defendants acts and practices with respect to the safekeeping of PII are negligent;

f. Award Plaintiff and members of the proposed Classes pre-judgment and post-judgment interest as permitted by law;

g. Award Plaintiff and members of the proposed Classes reasonable attorneys' fees and costs of suit; including expert witness fees; and

h. Award Plaintiff and members of the proposed Classes any further relief the Court deems proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial on all claims so triable.

Dated: September 5, 2019

Respectfully submitted,

/s/ Scott R. Drury
SCOTT R. DRURY

Michael Kanovitz
Scott R. Drury
LOEVY & LOEVY
311 N. Aberdeen, 3rd Floor
Chicago, Illinois 60607
312.243.5900
mike@loevy.com
drury@loevy.com